Google Inc. et al v. Egger et al Doc. 596 Att. 6

STATE OF VERMONT
PUBLIC SERVICE BOARD

Docket No. 7183

Petition of Eight Ratepayers for an investigation of possible disclosure of private telephone records without customers' knowledge or consent by Verizon New England Inc., d/b/a Verizon Vermont	))))

Docket No. 7192

Petition of Vermont Department of Public Service for an investigation into alleged unlawful customer records disclosure by Verizon New England Inc., d/b/a Verizon Vermont	)))

Order entered: 9/18/2006

ORDER ON MOTION TO DISMISS

SUMMARY

This Order denies Verizon's motion to dismiss these dockets. We have jurisdiction under state law to proceed in this matter, and it has not been shown that federal law preempts that jurisdiction. Nothwithstanding the many bases upon which Verizon asserts that the claims here are preempted by federal law and that all critical evidence is privileged or otherwise unavailable, we conclude that petitioners may still be able to adduce facts that sustain at least some of their claims. We recognize that discovery in this case may be limited, but we allow the petitioners to seek to prove their cases by whatever unprivileged evidence they can glean from discovery of Verizon and from whatever other reliable sources that may develop.

Based on the record before us, we conclude that the state secrets privilege does not apply here, largely because it has not been properly claimed, but also because it would not apply to all of petitioners' claims and because some of the matters involved in these dockets are not secret. We also conclude that dismissal is not required by the National Security Agency statute, the

Dockets.Justia.com

Foreign Intelligence Surveillance Act, the statutes and rules regarding classified information, or the Intelligence Reform and Terrorism Prevention Act of 2004.

Because of prior public disclosures by Verizon, we also specifically authorize the parties to conduct discovery on whether Verizon has provided local calling records to the NSA, whether Verizon provided information to the NSA before February, 2006, and the conditions under which Verizon provides others with access to its customer records.

Finally, we deny Mr. Michael Bandler's motion to establish a new schedule and we grant his motion to allow discovery regarding private "data brokers."

TABLE OF CONTENTS

I. Background 3
- The Petitions 3
- The Motions To Dismiss 6
- Responses to the Motion 8
- Participation by the United States Government 9
- Responses and Replies to the Department of Justice Letter 10

II. Discussion 12
- Standard for Motions to Dismiss 12
- State Law - Public Service Board Jurisdiction 13
- Federal Law 14
- State Secrets 14
  - Justiciability of Claims 14
  - Evidentiary Privilege 16
- Field Preemption 21
- Statutory Arguments 22
  - The NSA Statute 22
  - Foreign Intelligence Surveillance Act 24
  - Classified Iinformation 25
  - Intelligence Reform and Terrorism Prevention Act of 2004 27
- Other Procedural Motions 28

III. Conclusion 28

I. BACKGROUND

The Petitions

These cases were commenced to examine whether Verizon New England Inc., d/b/a Verizon Vermont ("Verizon"), had violated a variety of Vermont utility standards by directly or indirectly providing customer record information to the National Security Agency ("NSA") or other federal or state agencies ("NSA Customer Records Program"). Docket 7183 was initiated by a petition filed on May 24, 2006, by the American Civil Liberties Union of Vermont ("ACLU") and by seven individual ratepayers. Docket 7192 was initiated by petition of the Vermont Department of Public Service ("Department") filed on June 21, 2006.[1]

The petitions allege several violations of state utility law, rules or policy by Verizon:

1. By participating in the NSA Customer Records Program, Verizon violated Vermont Consumer Bill of Rights and Consumer Protection Standards that give customers control over the release of information regarding themselves and their calling patterns.[2]

2. By participating in the NSA Customer Records Program, Verizon violated a Vermont requirement that it take reasonable care to protect the privacy interests of its customers.[3]

---

1. The petitioners seek information about: (1) direct disclosure by Verizon of customer telephone records; (2) "occasions when customer records may have been obtained by state or federal officials without Verizon's consent;" and (3) opportunities for the NSA or other government agencies "to access Verizon customer records without Verizon's knowledge." Docket 7183 Petition at 3.

The petitioners also sought information from Verizon regarding similar disclosures to any other federal or state agency. In the text below , "NSA Customer Records Program" should be read as including disclosures to and activity by any state or federal agency, including but not limited to the NSA.

2. This standard was first established in a Board Order issued in 1999 and now is codified in Board Rule 7.605(A)(10) which provides customers with "[t]he right to privacy by controlling the release of information about oneself and one's calling patterns and by controlling unreasonable intrusions upon privacy."

3. *See* Rule 7.608(A)(1).

3. By participating in the NSA Customer Records Program without advance customer notice, Verizon committed an unfair marketing practice consisting of failing to follow privacy assurances previously given to its customers.[4]

4. By failing to file a privacy analysis statement with the Board before participating in the NSA Customer Records Program, Verizon violated applicable Consumer protection standards that require advance analysis of actions affecting customer privacy interests.[5]

5. Verizon violated 30 V.S.A. § 206 by providing misleading and inaccurate responses to inquiries from the Department. There are no allegations, either by petitioners or Verizon, that Verizon was coerced into participating in the NSA Customer Records Program. It has been reported that one major Bell company, Qwest, elected not to participate.[6]

The petitions raise the following questions of fact:

1. Did Verizon participate in the NSA Customer Records Program?

a. By directly disclosing customer information to the NSA and, if so, whether that disclosure was without legal authorization or beyond the scope of authorized business purposes?

---

4. The petition quotes Verizon as asserting "that it protects consumer safety, informs customers how their information is used and notifies consumers of changes that may affect their privacy interests." Docket 7183 Petition at 2.

5. This standard was first established in a Board Order issued in 1999. It is now codified in Board Rule 7.608(A)(2), which states:

> When or before a carrier files a tariff that introduces or modifies a service or implements a technology change that may affect the privacy interests of customers, the company shall file a privacy analysis statement with the Board and Department. The statement shall describe foreseeable changes to customer privacy protections and expectations. The statement shall also describe any privacy related actions the carrier proposes to take and options the carrier proposes to make available to customers.

6. According to counsel for Qwest's former Chief Executive Officer Joseph Nacchio, the government approached Mr. Nacchio several times between the fall of 2001 and the summer of 2002 to request its customer telephone records, but because the government failed to cite any legal authorization in support of its demands, Mr. Nacchio refused the requests. *See* John O'Neil, *Qwest's Refusal of N.S.A. Query Is Explained*, N.Y. Times, May 12, 2006. Quoted in *Terkel v. AT&T Corp.*, ___ F.Supp. ___, 2006 WL 2088202, slip op. at 23 (N.D.Ill. July 25, 2006) ("*Terkel*").

b. By allowing the NSA to obtain Verizon customer records without Verizon's consent or without Verizon's knowledge, such as by modifying its equipment or physical plant to grant the NSA access to data carried on Verizon's network?

2. If Verizon did participate:

a. Has Verizon received legal authorizations to participate in NSA Customer Records Program in the form of express customer consent, judicial warrants, properly issued subpoenas or valid "National Security Letters" or other forms of assurance from governmental officials regarding the legality of participating in the above NSA Customer Records Program?

b. Has Verizon received compensation?

c. Has Verizon provided accurate information to its customers?

d. Has Verizon provided accurate information to the Department?

3. How does Verizon record information requests from the NSA and its own responses?

Petitioners seek a variety of relief, including an order mandating individual customer notices describing past actions by Verizon, a decision to assign NSA Customer Records Program costs to shareholders rather than ratepayers, and financial penalties.

The NSA also operates a program that intercepts the contents of certain communications where one party to the communication is outside the United States and where the government has a reasonable basis to conclude that one party to the communication has a relationship with al Qaeda.[7] One federal court has held that this content interception program violates the Administrative Procedures Act, the Separation of Powers Doctrine, the First and Fourteenth Amendment, and statutory law.[8] This content interception program is not in issue here.

---

7. This program was announced by President Bush and Attorney General Gonzalez in late 2004. *See* http://www.whitehouse.gov/news/releases/2005/12/print/20051219 1.html.

8. *American Civil Liberties Union v. National Security Agency*, ___ F.Supp. ____ slip op. at 2 (E.D. Mich., Aug. 17, 2006) ("*ACLU v. NSA*").

The Motions To Dismiss

On June 30, 2006, Verizon filed a Motion to Dismiss ("MTD") in each docket. Verizon's motions argued that the Board's jurisdiction over this matter has been preempted by federal law and programs. Verizon contended that: (1) because of varying federal limitations on the Board's ability to develop evidence in these dockets, the Board will be unable to adduce any facts relating to the subject matter of the petitions and thus will be unable to resolve the issues; and (2) any potential relief would implicate issues of national security and is beyond the Board's power to grant. Verizon also argued that the United States Government ("USG") has written to officials in other states asserting that the contents of the NSA Customer Records Program is subject to a security classification and that any subpoena response that disclosed the details of the program would harm the national security and is therefore preempted by federal law. Because the relevant information is classified, Verizon asserted, its officials might subject themselves to criminal penalties by complying with a discovery request. In sum, Verizon contended that the Board cannot expect to receive evidence other than newspaper articles to evaluate the petitioners' claims and should dismiss for that reason.

Verizon also argued that proceeding further in these dockets would require Verizon to violate federal law, thereby creating an explicit conflict that mandates federal preemption. In this regard, Verizon raises two federal statutes. Verizon cited a provision of the National Security Act which says that no law may require disclosure of any information with respect to the activities of the NSA.[9] It also cited portions of the Foreign Intelligence Surveillance Act.[10]

Verizon also noted that the United States Department of Justice has raised the state secrets privilege in other similar proceedings. Verizon asserted that this privilege is "an absolute bar to disclosure and no competing public or private interest can be advanced to compel disclosure."[11] Also, Verizon reported that the state secrets privilege bars any action where the plaintiff cannot develop a prima facie case or the defendant would be barred from establishing a valid defense.

---

9. *See* 50 U.S.C. § 402.
10. *See* 50 U.S.C. § 1805(c)(2)(B) and (C).
11. Verizon motion at 6, quoting from *Ellsberg v. Mitchell*, 709 F.2d 51, 57 (D.C. Cir. 1983).

Verizon's motion also made factual assertions regarding its past practices and current policies. Verizon said it "can neither confirm nor deny whether it has any relationship to the classified NSA program."[12] Nevertheless, Verizon also asserted that it has not turned over local calling records to the NSA.[13] In an attached news release dated May 16, 2006, Verizon also made a broader denial:

> One of the most glaring and repeated falsehoods in the media reporting is the assertion that, in the aftermath of the 9/11 attacks, Verizon was approached by NSA and entered into an arrangement to provide the NSA with data from its customers' domestic calls.
>
> This is false. From the time of the 9/11 attacks until just four months ago, Verizon had three major businesses – its wireline phone business, its wireless company and its directory publishing business. It also had its own Internet Service Provider and long-distance businesses. Contrary to the media reports, Verizon was not asked to provide, nor did Verizon provide, customer phone records from any of these businesses, or any call data from those records. None of these companies – wireless or wireline – provided customer records or call data.[14]

We understand this to be a denial that Verizon had provided any call record information to the NSA until approximately February, 2006, four months before the press release. However, we note that it also leaves open the possibility that Verizon, while not actively passing on customer records and call data, nonetheless made it possible for the NSA to obtain that information.

In another press release issued on May 12, 2006, Verizon also asserted that it:

> will provide customer information to a government agency only where authorized by law for appropriately-defined and focused purposes. When information is provided, Verizon seeks to ensure it is properly used for that purpose and is subject to appropriate safeguards against improper use. Verizon does not, and will not, provide any government agency unfettered access to our cusomer records or provide information to the government under circumstances that would allow a fishing expedition.[15]

Verizon's motion similarly asserted that to the extent it provides assistance to the government for national security or other purposes, it will provide customer information to a government agency

12. Verizon MTD at 4.
13. Verizon MTD at 4.
14. Verizon MTD, exh. 8.
15. Verizon MTD, exh. 9.

only where authorized by law for appropriately-defined and focused purposes.[16] In addition, Verizon explained that under certain federal statutes, it must disclose information when it receives a "national security letter" or a "specified certification" from the government.

Verizon concludes that the Vermont Public Service Board is not the appropriate forum to resolve the issues here. Rather, Verizon asserted, Congressional oversight and pending federal court proceedings are more appropriate venues.[17]

Responses to the Motion

On July 21, 2006, the Department, the ACLU and Mr. Barry Kade all filed responses.

The Department argued that neither the details nor the propriety of classified national security programs or the workings of the NSA are at issue here. Rather, the Department contended that the "petitioners in both dockets have as their primary concern the privacy of Verizon's Vermont customers and the company's compliance with state and federal privacy laws."[18] The Department also argued that Verizon has not demonstrated preemption and that the motion should be denied because in a motion to dismiss the petitioners' assertions should be taken as true. The Department also contended that several issues in these dockets, such as utility record-keeping and the adequacy of past Verizon responses to discovery requests, are not preempted.

ACLU argued that this Board is the proper body under state law to decide the petitions and that the issues can be decided solely on state law grounds, and without any reference to federal issues. ACLU contended that the Board need not inquire whether Verizon has any relationship to or cooperated with a classified NSA program. ACLU also cited the standard of review for motions to dismiss for failure to state a claim.

Mr. Barry Kade argued that the Board has no jurisdiction to evaluate federal issues such as those raised by "the State Secrets Act" or other federal laws cited by Verizon. He also argued that granting the motion to dismiss would violate the oath of office taken by the Board's members.

---

16. MTD at 4.
17. There is no pending federal court case involving the phone records of Vermont customers.
18. DPS response at 1.

On July 28, Verizon filed a reply maintaining its earlier position that the Board lacks jurisdiction "in the national security area."[19] Verizon also discussed recent decisions on similar issues by the FCC, federal courts and other state commissions, and it provided photocopies of documents filed in various state and federal fora. Verizon also argued that supervision of intelligence activities is more appropriately conducted by Congress.

Participation by the United States Government

In a procedural order issued on July 12, 2006, we invited the USG to intervene in these dockets. We observed that the state secrets privilege, a possible defense by Verizon, had been raised, but that the privilege:

> belongs to the Government and must be asserted by it. It can neither be claimed nor waived by a private party. If the USG is not present in this case, it may not be possible to consider Verizon's argument, and the interests of the USG may be harmed.[20]

On July 31, 2006, the United States Department of Justice filed a letter on behalf of the USG ("DOJ letter"). The USG declined to intervene and asserted that its letter should not be deemed to be a "submission of the United States to the jurisdiction of Vermont."

Nevertheless, the DOJ letter takes a substantive position on the pending Motion to Dismiss. It argues generally that:

> the request for information and the application of state law they embody are inconsistent with and preempted under the Supremacy Clause, and that compliance with [the Department's Document Requests], and any similar discovery propounded by the [Board], would place [Verizon] in a position of having to confirm or deny the existence of information that cannot be confirmed or denied without harming national security.[21]

The DOJ letter offers several legal grounds for preemption.

1. It argues that providing the requested information would interfere with the Nation's foreign-intelligence gathering, a field reserved exclusively to the Federal Government.[22]

---

19. Verizon reply at 4.

20. Order of July 12, 2006, at 3 (footnote omitted).

21. DOJ letter at 7.

22. DOJ letter at 3.

2. It argues that providing the requested information would violate various statutes, including the National Security Agency Act and the Intelligence Reform and Terrorism Prevention Act of 2004 as well as statutes and executive orders relating to classified information.[23]

3. It mentions, but does not clearly assert, the state secrets privilege. For example, the letter notes that court decisions on similar matters in another case "underscores that compliance with the requests for information would be improper."[24] The closest thing to a claim of privilege in the letter is an assertion that the state secrets privilege "covers the precise subject matter sought from [Verizon] by Vermont officials.[25]

The DOJ letter did not include any affidavits or sworn statement prepared for these dockets. It did include a photocopy of an affidavit submitted in a federal court proceeding by the Director of National Intelligence ("DNI") and asserting the state secrets privilege.[26]

Responses and Replies to the Department of Justice Letter

Both the ACLU and the Department filed responses to the DOJ letter. They both note that the USG has declined to intervene, and they argue that the Board should disregard the DOJ letter. The ACLU states that the government "cannot at once assert its interest in the case and separate itself from the proceedings."[27] Both also argue that even where a state secrets privilege is asserted, the Board should carefully analyze whether the current circumstances warrant application of the privilege.

Both also argue that the DOJ letter addressed only some of the issues in this docket. The Department specifically mentioned Verizon's practices regarding "maintaining and protecting private customer information, and whether [Verizon has] violated Vermont or federal disclosure

---

23. DOJ letter at 4-5.
24. DOJ letter at 5.
25. DOJ letter at 6.
26. DOJ letter, attachments from July 28 FAX at 16-17 (Negroponte statement at 4-5).
27. ACLU response at 2.

laws, or [Verizon's] own policies."[28] For example, the Department asserts that Verizon could, consistent with its asserted privilege, answer a question about whether it has:

> disclosed any customer information that is deemed protected under state or federal law to any state or federal agency in the absence of a warrant, subpoena, court order or other applicable written authorization . . . .[29]

ACLU also contends that the DOJ letter objected solely to the DPS's discovery in Docket No. 7192, and not to discovery by the ACLU or individual petitioners in Docket No. 7183. Finally, ACLU argues that "the fact that Verizon will neither confirm nor deny its cooperation with the NSA is evidence, in and of itself, that Verizon has violated Vermont's Consumer Protection Standards"[30] as well as Verizon's own stated privacy principles. The Department also contends that Verizon has made numerous public statements regarding these matters that moot any claim of privilege.

On August 15, Petitioner Michael Bandler filed a "Notice of Omnibus Relief" seeking to suppress the response from the USG or to set a revised schedule allowing Petitioners to respond to the USG papers. He argued that the USG "must be either in or out. It must submit to the authority of the Board or be silent . . . ."[31] Mr. Bandler also reported that the DOJ letter had not been sent to the service list in these dockets, and he asked for appropriate relief including a new schedule after the DOJ letter is served on the parties.

Verizon filed a reply letter on August 23, 2006, asserting that other parties had failed to address the central issue. Verizon disagrees with the ACLU on the scope of the questions allowable if the state secrets privilege applies. Verizon contends that USG lawsuits filed in federal district courts in other states demonstrate that the USG's claims apply broadly to all discovery on matters relating to the NSA Customer Records Program. Verizon also disagrees with ACLU's claim that the Board should determine the scope of any asserted privilege. Citing several recent decisions, Verizon argues that only the federal courts may make such a determination of the scope of the privilege. Verizon also disagrees with ACLU's argument that

28. Department response at 2.
29. Department response at 2.
30. ACLU response at 3.
31. Bandler letter at 3.

its customer disclosures are inadequate. Verizon says those statements "make clear that Verizon will provide customer information in response to lawful requests or as a result of safety considerations."[32] Verizon also disagrees with the Department's assertion that some discovery could survive the recognition of a state secrets privilege. Verizon asserts that it has "already responded to the DPS's requests insofar as they sought general information – it objected only to those requests that sought information concerning its alleged cooperation with the NSA."[33] Finally, Verizon disagrees that its past disclosures had mooted any privilege claims; it contends that only the government can waive this privilege.

On August 25, 2006, Petitioner Bandler also filed a letter reviewing recent federal district court decisions. He argued that Verizon's press releases have eliminated any secrecy involved in the NSA Customer Records Program. He also attached photocopies of various news stories discussing "data brokers" which are private entities who reportedly are able to collect phone records and provide them to police agencies. Mr. Bandler asks that the Board expand the scope of these dockets to include investigation of data brokers.

II. Discussion

Standard for Motions to Dismiss

We construe Verizon's Motion to Dismiss as a Motion For Judgment on the Pleadings under Civil Rule 12(c).[34] To grant Verizon's motion, this Board must take as true all well-pleaded factual allegations in the petition and all reasonable inferences drawn from those allegations. We must take as false all contravening assertions in Verizon's pleadings. We may grant the motion only if the petitions contain no allegations that, if proven, would permit

32. Verizon letter at 3.

33. Verizon letter at 3.

34. Verizon did not cite Rule 12(c), but this decision is not incompatible with the motion. By applying Rule 12(c), Verizon gains the opportunity to have us consider the motion as a motion for summary judgment, and thus to consider more than the pleadings.

recovery.[35] To prevail, Verizon must show "beyond doubt that there exist no facts or circumstances that would entitle the [petitioners] to relief."[36]

State Law – Public Service Board Jurisdiction

As a matter of state law, the Board has jurisdiction over the claims asserted in the petitions. Verizon is a company offering telecommunications services on a common carrier basis in Vermont, and it therefore is a utility subject to the Board's jurisdiction.[37] That jurisdiction extends to the manner of operating and conducting that business, so as to ensure that the service is reasonable and expedient, and to "promote the safety, convenience and accommodation of the public."[38] The Board has broad supervisory jurisdiction over Verizon's operations in Vermont.[39] As to matters within its jurisdiction, the Board has the same authority as a court of record.[40] In addition, the Board has authority to impose civil penalties for an improper refusal to provide information to the Department or for violating a rule of the Board.[41]

The privacy of customer information has earned special mention in Vermont statutes. For example, when the Board considers a plan for alternative regulation of telecommunications companies, it must consider privacy issues.[42] Moreover, by accepting an alternative form of regulation pursuant to 30 V.S.A. § 226b, Verizon has acknowledged the Board's authority to set boundaries on Verizon's policies affecting customer privacy.[43]

The Board's authority arises solely from statute, and it does not have jurisdiction over every claim that may involve a utility. For example, the Supreme Court has held that the Board

35. *Knight v. Rower*, 170 Vt. 96 (1999).

36. *Union Mutual Fire Ins. Co. v. Joerg*, 2003 VT 27, 4, 824 A.2d 586, 588 (2003); Amy's *Enterprises v. Sorrell*, 174 Vt. 623, 623 (2002)(mem.).

37. 30 V.S.A. § 203(5).

38. 30 V.S.A. § 209(a)(3).

39. *In re Verizon New England, Inc.*, 173 Vt. 327, 334-35 (2002).

40. 30 V.S.A. § 9.

41. 30 V.S.A. § 30.

42. *See* 30 V.S.A. §§ 226a(c) and 226(c)(8).

43. *In re Verizon New England, Inc.,* Docket No. 6959 and 7142, Order of 4/27/06, App. A, §§ II.B.(c)(7), III.B.

has no jurisdiction over certain traditional torts merely because the defendant is a utility.[44] Verizon's motion, however, is not based upon any such limitation in state law.

Federal Law

Verizon's central contention is that federal law preempts matters that otherwise would be within the jurisdiction of the Board under state law.[45] The ACLU argues, to the contrary, that "federal law and issues of national security need not be addressed" here. Petitioner Kade agrees with the ACLU and further argues that the Board not only has no jurisdiction to evaluate federal law but that its members are prevented by their oaths of office from evaluating such issues.

We agree with Verizon. The ACLU and Mr. Kade misapprehend the Board's duty regarding federal law. The supremacy clause of the United States Constitution allows federal law to preempt fully state and local laws.[46] In ruling on matters within our jurisdiction, we must consider whether federal law has preempted our state jurisdiction and yield if we find such preemption.

It is also true, however, that this Board ordinarily applies state law until it finds that it has been preempted. Preemption can be established in a number of ways, including explicit or implicit statutory language, actual conflict, or occupation of the field.[47] Therefore, we undertake below to evaluate each of the theories advanced by Verizon as a basis for preemption.

State Secrets

The broadest challenge to the Board's jurisdiction is that these dockets involve state secrets. The state secrets privilege contains two distinct lines of cases.

Justiciability of Claims

The first line of cases is essentially a rule of "non-justiciability" that deprives courts of authority to hear suits against the Government based on certain espionage or intelligence-related

---

44. *E.g., Trybulski v. Bellows Falls Hydro-Elect. Corp.*, 112 Vt. 1 (1941) (Board did not have jurisdiction to assess damages for injuries to private landowners' properties allegedly caused by improper maintenance and operation of dam by hydro-electric company).

45. *See, e.g.* Verizon MTD at 3, note 1 ("state agencies lack jurisdiction with respect to matters relating to Verizon's alleged cooperation with federal national security or law enforcement authorities.")

46. U.S. Const. art. VI, cl. 2; *Crosby v. National Foreign Trade Council*, 530 U.S. 363, 372, 120 S.Ct. 2288, 147 L.Ed.2d 352 (2000).

47. *See, e.g., In re Verizon New England, Inc.*, 173 Vt. 327, 336 (2002).

subjects. The seminal decision in this line of cases is the 1875 decision in *Totten v. United States*.[48] The plaintiff in that case brought suit against the government seeking payment for espionage services he had provided during the Civil War. The Court's decision noted the unusual nature of a contract for espionage:

> The service stipulated by the contract was a secret service; the information sought was to be obtained clandestinely, and was to be communicated privately; the employment and the service were to be equally concealed. Both employer and agent must have understood that the lips of the other were to be for ever sealed respecting the relation of either to the matter. This condition of the engagement was implied from the nature of the employment, and is implied in all secret employments of the government in time of war, or upon matters affecting our foreign relations, where a disclosure of the service might compromise or embarrass our government in its public duties, or endanger the person or injure the character of the agent.[49]

Given the unusually secret nature of these contracts, the Court held that no action was possible for their enforcement. Indeed, "[t]he publicity produced by an action would itself be a breach of a contract of that kind, and thus defeat a recovery."[50]

The Supreme Court recently reaffirmed this principle in *Tenet v. Doe*.[51] In *Tenet*, the plaintiffs, who were former Cold War spies, brought estoppel and due process claims against the United States and the Director of the Central Intelligence Agency for its alleged failure to provide them with the assistance it had allegedly promised in return for their espionage services.[52] Relying heavily on *Totten*, the Court held that the plaintiffs claims were barred. For a unanimous Court, Chief Justice Rehnquist wrote:

> We adhere to *Totten*. The state secrets privilege and the more frequent use of in camera judicial proceedings simply cannot provide the absolute protection we found necessary in enunciating the Totten rule. The possibility that a suit may proceed and an espionage relationship may be revealed, if the state secrets privilege is found not to apply, is unacceptable. Even a small chance that some

48. 92 U.S. 105 (1875).
49. *Totten*, 92 U.S. at 106.
50. *Totten*, 92 U.S. at 107.
51. *Tenet v. Doe*, 544 U.S. 1, (2005).
52. *Tenet* at 3.

> court will order disclosure of a source's identity could well impair intelligence gathering and cause sources to 'close up like a clam.'[53]

The *Totten/Tenet* principle, where applicable, provides an absolute bar to any kind of judicial review, and therefore would also bar any quasi-judicial proceeding by a state agency.[54]

The *Totten/Tenet* rule is inapplicable here. It applies to actions where there is a secret espionage relationship between the Plaintiff and the Government.[55] Petitioners here do not claim to be spies or to have any form of secret espionage relationship with the government. Therefore the absolute bar rule does not apply to these dockets.

Evidentiary Privilege

The second branch of the state secrets doctrine deals with the exclusion of evidence, and the consequences of that exclusion.

The effect of the state secrets privilege on plaintiffs is like other evidentiary privileges. Where a privilege blocks admission of some evidence, a plaintiff nevertheless may use other evidence to prove his or her case. However, if the plaintiff fails to carry its burden of proof, the court may dismiss the case or grant summary judgment against the plaintiff, as in any other proceeding.[56]

For defendants, the state secrets privilege produces the opposite of the normal result. Normally a defendant who needs privileged evidence admitted into evidence is harmed by the privilege. With the state secrets privilege, however, the defendant gains an advantage. Where a defendant needs evidence comprising a state secret in order to create a valid defense, summary judgment must be granted to the defendant.[57]

---

53. *Tenet* at 11 (citations omitted).

54. *Tenet* at 8.

55. *Tenet* at 7-8; *ACLU v. NSA* at 10-11; cf. *Terkel*at 15-16 (declining to extend *Totten* principle to disclosure of telephone records to the government because such disclosures are not inherently harmful to national security and would reveal violations of plaintiffs' statutory rights).

56. *United States v. Reynolds*, 345 U.S. 1, 11 (1953); *Kasza v. Browner*, 133 F.3d 1159, 1166 (9th Cir. 1998); *Ellsberg v. Mitchell*, 709 F.2d 51, 57 (D.C.Cir. 1983).

57. *Kasza*, 133 F.3d at 1166; *Bareford v. General Dynamics Corp.*, 973 F.2d 1138, 1141 (5th Cir. 1992). Normally a defendant relying on privileged evidence would be deprived of that evidence, and might thereby lose a valid defense. However, by requiring dismissal in such cases, the state secrets privilege uniquely operates to benefit defendants in all cases, regardless of which party needs the secret evidence.

For three independent reasons, we deny the Motion to Dismiss on grounds of the state secrets privilege.

1. Verizon has not properly invoked the privilege

The United States Supreme Court has explained that the state secrets "privilege belongs to the Government and must be asserted by it; it can neither be claimed nor waived by a private party. Moreover, there must be a "formal claim of privilege, lodged by the head of the department which has control over the matter, after actual personal consideration by that officer."[58]

Here, the government has declined to become a party, despite our earlier invitation to do so.[59] Verizon is a party, but under federal law it does not have standing to raise the privilege. Moreover, no party has submitted any sworn statement prepared for these dockets. Instead, both Verizon and the DOJ letter included photocopies of affidavits filed in other proceedings by the Director of National Intelligence.[60]

A motion to dismiss may be treated as a motion for summary judgment if it involves matters outside the pleadings.[61] Since the DOJ letter is not a pleading, we could grant summary judgment for Verizon if the record shows that there are no material facts that are genuinely in dispute. Partial summary judgment can also be granted when only some issues are in dispute.[62] Summary judgment can be granted without affidavits,[63] but affidavits can be used to show that no material issue of fact exists. Where affidavits are submitted, they must be based upon personal knowledge.[64]

---

58. *United States v. Reynolds*, 345 U.S. 1, 7-8 (1953); *Hepting v. AT & T Corp.*, ___ F.Supp. ___, 2006 WL 2038464, slip op. at 16 (N.D. Cal. June 20, 2006) ("*Hepting*").

59. As noted above, the Department of Justice declined to intervene and asserted that its letter should not be deemed to be a "submission of the United States to the jurisdiction of Vermont." We are puzzled by this statement because we are not aware that when the United States intervenes in a state administrative proceeding the form gains "jurisdiction" over the federal government.

60. *E.g.,* DOJ letter, attachments from July 28 FAX at 16-17 (Negroponte statement at 4-5).

61. V.R.C.P. 12(c).

62. V.R.C.P. 12(d). Summary judgment cannot be granted, however, without offering the parties a reasonable opportunity to present material pertinent to the motion. V.R.C.P. 12(c).

63. V.R.C.P. 56(b).

64. V.R.C.P. 56(e); *Department of Social Welfare v. Berlin Development Assoc.*, 138 Vt. 160 (1980).

We noted above that federal law requires the government to claim the state secrets privilege. This is not an empty formality. Because the privilege, once accepted, creates an absolute bar to the consideration of evidence, the courts do not lightly accept a claim of privilege. In each case, the government's showing of necessity for the privilege determines "how far the court probes in satisfying itself that the occasion for invoking the privilege is appropriate."[65] The courts have made it clear that "control over the evidence in a case cannot be abdicated to the caprice of executive officers.[66] The privilege may not be used to shield any material not strictly necessary to prevent injury to national security; and, whenever possible, sensitive information must be disentangled from nonsensitive information to allow for the release of the latter.[67]

Federal courts have frequently conducted *in camera* proceedings to test the assertion of the privilege.[68] In a recent Illinois case, the government has voluntarily filed both public and secret *in camera* affidavits for the court's consideration.[69] We recognize that *in camera* proceedings before this Board may present difficulties that do not arise in federal courts. However, we understand the relevant federal law to require not only that the privilege be claimed by the responsible official but that the trier of fact at least minimally test whether "the occasion for invoking the privilege is appropriate."[70] We are not convinced that those difficulties cannot be overcome.[71]

The privacy issued raised in these dockets are of great interest to Vermont ratepayers, and we are not willing to dismiss this proceeding without, at minimum, affidavits sufficient to justify that action. Therefore we hold that the government's claim of privilege must be accompanied by at least some admissible evidence, ordinarily by affidavit, from a responsible official who asserts after personal consideration that the subject matter is a state secret.[72] No such affidavit has been

---

65. *U.S. v. Reynolds*, 345 U.S. at 11.
66. *U.S. v. Reynolds*, 345 U.S. at 11.
67. *Ellsberg v. Mitchell*, 709 F.2d 51, 56 (D.C. Cir. 1983).
68. *E.g., Hepting* at 4; *Terkel*at 5, 21.
69. *Terkel*at 5. The DOJ letter here attached a photocopy of the affidavit from *Terkel*.
70. *U.S. v. Reynolds* at 11.
71. *See* discussion below of CIPA rules for sharing of classified information in "graymail" cases.
72. *See, e.g., Hepting*at 16 (state secret privilege requires a formal claim by agency head after personal consideration).

submitted in this proceeding. Therefore the state secrets privilege has not been properly claimed here.

2. The state secrets privilege, if it did apply, would not bar all pending claims.

If petitioners cannot prove that Verizon has participated in the NSA Customer Records Program, petitioners may still be entitled to some relief here.

For example, they may request the Board to order Verizon to modify its existing customer privacy notices to describe the policies that Verizon would apply in the *hypothetical* event that Verizon is asked in the future to disclose confidential customer information pursuant to a secret government program. Even if this Board cannot consider what *has* happened, we are not preempted from requiring Verizon to provide notice to customers describing how Verizon would apply the known structures of federal law to government requests for otherwise private information.[73]

The Department has also asked to know more about the general standards that Verizon uses when it receives a request for cooperation from the United States government and how it records both such requests and its own responses. Verizon has asserted that "to the extent it provides assistance to the government for national security or other purposes, it will provide customer information to a government agency only where authorized by law for appropriately-defined and focused purposes."[74] The parties may legitimately seek more information regarding Verizon's beliefs about when government purposes are "appropriately-defined and focused." In addition, Verizon has explained that under certain federal statutes, it must disclose information when it receives a "national security letter" or a "specified certification."[75] The parties here may legitimately seek more information on when Verizon believes such letters and certifications are required and when, if ever, they are not required. These facts also might appropriately influence the content of customer notices and the company's written privacy policies.

---

73. This point is underscored by the breadth of the claims in Verizon's filings and in the DOJ letter. Those documents demonstrate that, regardless of what Verizon has done in the past, if it were to agree in the future to provide the NSA with customer record information, Verizon would consider itself barred from disclosing that fact.

74. Verizon MTD at 4.

75. Verizon MTD at 8, note 4.

Also, the state secrets privilege, even if it did apply, would not block consideration of whether Verizon's responses to the Department were misleading and inaccurate. As noted above, for purposes of a motion to dismiss, allegations in a petition are taken as true.[76]

3. Some of the facts are no longer secret.

We noted above that, on the one hand, Verizon has said that it "can neither confirm nor deny whether it has any relationship to the classified NSA program."[77] Yet Verizon also has on several occasions made carefully worded denials.

It is true, as Verizon asserts, that the state secrets privilege can be waived only by the government. However, non-governmental actors can alter what is a secret. In litigation over similar NSA programs in the Federal District Court for Northern California, the court denied a motion to dismiss. The court sensibly ruled that "the first step in determining whether a piece of information constitutes a 'state secret' is determining whether that information actually is a 'secret.'"[78] Where information that has been given to the public is accurate, this rule avoids improperly declaring as state secrets information that is not a secret at all. Where information that has been given to the public is inaccurate, this rule gives the courts the opportunity to correct the inaccurate reports.

As have the federal courts, we rely only on publicly reported information that bears persuasive indications of reliability.[79] As did Judge Walker in the *Hepting* case, we consider reliable any admissions by Verizon as to whether it has participated in the NSA Customer Records Program.

Verizon has asserted that it has *not* turned over local calling records to the NSA.[80] It also has denied having any relationship with the NSA before approximately February, 2006.[81]

---

76. If the Department cannot later develop evidence necessary to proceed to hearings, a motion for summary judgment may be appropriate.

77. Verizon MTD at 4.

78. *Hepting* at 18.

79. *Terkel* at 25; *Hepting* at 13.

80. Verizon MTD at 4.

81. Verizon's Motion to Dismiss, exhibit 8 included a press release dated May 16, 2006. It stated:

> "One of the most glaring and repeated falsehoods in the media reporting is the assertion that, in the aftermath of the 9/11 attacks, Verizon was approached by NSA and entered into an arrangement to provide the NSA with data from its customers' domestic calls.

(continued...)

Finally, it has asserted that it does not provide any government agency with "unfettered access" to its customer records and does not allow any "fishing expedition" into its records.[82] We understand these statements as partial denials of participation in the NSA program. As to information covered in these public statements, there is no longer any secret to which a privilege might attach.[83] Therefore, the parties in these Dockets may seek evidence on whether Verizon has provided local calling records to the NSA, whether Verizon provided information to the NSA before February, 2006, and the conditions under which Verizon provides access to its customer records.

Field Preemption

The USG argues that providing the requested information would interfere with the Nation's foreign-intelligence gathering, a field reserved exclusively to the Federal Government.[84] In short, the USG argues: (1) the field of foreign-intelligence gathering has been fully preempted; and (2) this prevents any and all state inquiry into communications between Verizon and the NSA that the USG describes as part of the USG's foreign-intelligence gathering efforts. While the first proposition above may be true, the second requires proof.

We reject the field preemption argument for procedural reasons. As we noted above, the USG has not appeared in this proceeding and has not offered any sworn evidence supporting its position. Instead, it has provided photocopies of affidavits it submitted in other proceedings. It

---

81. (...continued)
"This is false. From the time of the 9/11 attacks until just four months ago, Verizon had three major businesses – its wireline phone business, its wireless company and its directory publishing business. It also had its own Internet Service Provider and long-distance businesses. Contrary to the media reports, Verizon was not asked to provide, nor did Verizon provide, customer phone records from any of these businesses, or any call data from those records. None of these companies – wireless or wireline – provided customer records or call data."

82. Verizon's Motion to Dismiss, exhibit 9 was a press release dated May 12, 2006. In it Verizon asserted that it:
"will provide customer information to a government agency only where authorized by law for appropriately-defined and focused purposes. When information is provided, Verizon seeks to ensure it is properly used for that purpose and is subject to appropriate safeguards against improper use. Verizon does not, and will not, provide any government agency unfettered access to our customer records or provide information to the government under circumstances that would allow a fishing expedition."

83. *See Terkel* at 25. We also note more controversial authority stating that state secrets may be waived if they are widely reported in the press. *Spock v. United States*, 464 F.Supp. 520 (S.D.N.Y. 1978).

84. DOJ letter at 3.

is not enough, as the USG asserts, that a high government official recently told a federal court in another state that this subject involves national security.

Statutory Arguments

The NSA Statute

Verizon and the DOJ letter assert that Section 6(a) of the National Security Agency Act of 1959 ("NSA Statute") requires dismissal. This statute provides:

> Sec. 6. (a) . . . [N]othing in this Act or any other law . . . shall be construed to require the disclosure of the organization or any function of the National Security Agency, of any information with respect to the activities thereof, or of the names, titles, salaries, or number of the persons employed by such agency.[85]

On its face, this statute is extraordinarily broad. By its terms, it trumps *any* "other law," state or federal. One federal court, commenting on the breadth of this statute observed that if this statute were:

> taken to its logical conclusion, it would allow the federal government to conceal information regarding blatantly illegal or unconstitutional activities simply by assigning these activities to the NSA or claiming they implicated information about the NSA's functions.[86]

Courts have nevertheless applied the statute as written. For example, the statute gives the NSA the absolute right to resist a Freedom of Information request seeking disclosure of information from the NSA's own files regarding its own operations.[87]

Verizon's interpretation would further expand the reach of the statute. Verizon argues: (1) it may have provided information to the NSA; and (2) requiring it to now explain what it did would improperly disclose the activities of the NSA.

This interpretation not only protects NSA employees, officers and files from forced disclosures, but it would also apply the statute to people with whom NSA has had contact and from whom it has requested information. The argument seems to be a form of "Midas Touch" for the NSA: anything it touches becomes secret. Once the USG has asserted that the activities of *any* private person also relate to NSA activities, the USG's argument seems to require that the

85. Pub. L. No. 86-36, § 6, 73 Stat. 63, 64, codified at 50 U.S.C. § 402 note.

86. *Terkel* at 11.

87. *Id.*; *Hayden v. National Security Agency*, 608 F.2d 1381 (D.C. Cir. 1979).

activity as a whole becomes privileged and all state inquiry about that activity must cease, regardless of the consequences to petitioners, respondents, utilities and customers. This goes far beyond the scope of a statute nominally aimed at keeping confidential the names, salaries and activities of NSA employees. Moreover, courts have made clear that a simple assertion that Section 6(a) applies is inadequate. For example, in *Founding Church of Scientology v. NSA*, the Court of Appeals for the District of Columbia rejected the District Court's reliance upon an affidavit from the NSA invoking Section 6 when that affidavit made simple conclusory assertions which were not substantiated.[88] Here, Verizon has simply made broad assertions, unsupported by an affidavit by the NSA. Therefore, we conclude that Verizon has not presented a sufficiently detailed basis for us to find that Section 6(a) bars disclosure of all information that may be relevant to this proceeding.

Even though the courts have applied Section 6(a) broadly, for an independent reason it does not support dismissal at this time. In the *Hepting* case in Northern California, Judge Walker denied dismissal of similar claims, even though he blocked discovery on those same claims. He noted the possibility that the government or the defendant telecommunications carrier might make public disclosures that would support the claims made in that case. Instead of dismissing the case, the judge offered to make step-by-step determinations during discovery as to whether the various privileges would prevent plaintiffs from discovering evidence.[89]

We have decided to follow the same course. Verizon or other utilities who participated in the NSA Customer Records Program may make further disclosures that are sufficiently reliable to alter the outcome. Although some of the petitioners' discovery requests may be blocked by one or another privilege, some information about Verizon's activities may nevertheless emerge. Later, Verizon might be entitled to summary judgment if the state secrets privilege blocks certain items of evidence that are essential to plaintiffs' prima facie case or to Verizon's defense. Alternatively, time may provide petitioners more non-classified and admissible materials, and it is at least conceivable that some of petitioners' claims could survive summary judgment. As discovery proceeds, we will be willing to determine step-by-step whether the privilege prevents

88. 610 F.2d 824, 831–833 (1978).

89. *Hepting* at 21.

petitioners from discovering particular evidence. The mere existence of the NSA statute, however, does not justify dismissing these dockets now.

Foreign Intelligence Surveillance Act

Verizon asserts that it is prohibited from providing information by a provision of the Foreign Intelligence Surveillance Act ("FISA").[90] These statutes relate to the terms of judicial FISA orders authorizing electronic surveillance. They allow a court issuing a surveillance warrant to direct a common carrier to cooperate in executing that warrant and also to direct that the carrier protect the secrecy of the surveillance while minimally interfering with the target's normal services.[91] The statutes also allow the court to require the carrier to keep records of the surveillance.[92]

These statutes are irrelevant. Nothing in the record suggests that Verizon ever received a FISA warrant regarding the NSA Customer Records Program.

As noted above, the federal government operates a program of warrantless interception of certain communications involving persons suspected of having contacts with al Qaeda has recently been reviewed in the courts. One court has held that this program violates FISA because the program "has undisputedly been implemented without regard to FISA."[93] If the United States government operates its content interception program without recourse to FISA, we see little reason to infer that it would use those procedures to obtain disclosure of telecommunications records.

Classified Information

Verizon also moves to dismiss on the grounds that if it has participated in the NSA Customer Records Program, that program, and Verizon's participation, would be classified information. As a result, if Verizon were required to provide such information it would be

90. Verizon MTD at 5.
91. 50 U.S.C. § 1805(c)(2)(B).
92. 50 U.S.C. § 1805(c)(2)(C).
93. *ACLU v. NSA* at 2.

subject to prosecution for a felony.[94] Therefore, Verizon argues that the federal classification imposes conflicting state and federal duties, in which the federal duty must be supreme.

The DOJ letter asserts that various Executive Orders require that classified information cannot be disclosed unless the head of the agency imposing the classification has authorized disclosure, the recipient has signed a nondisclosure agreement, and the person has a need-to-know.[95] According to the DOJ, Vermont state officials do not qualify.

Initially, we note that the DOJ letter suggests that a very broad category of information is classified. The DOJ letter asserts the claim for any and all matters relating to the "foreign-intelligence activities of the United States."[96] Given the context, however, this also includes domestic data collection activities. In this sense, the USG defines "foreign-intelligence" by the purpose of the activity, not the location at which the information is collected.

We also note that this dispute does not involve a party seeking disclosure of information held in government files or a party seeking to compel the testimony of a government official or employee. Instead, the alleged classified activity involves the activities of civilian employees of a telecommunications company regulated in Vermont. The petitioners assert that Verizon may have transferred data to the government or even given the government access to customer information and calling patterns contained in the utility's files. Therefore what is putatively classified here is the knowledge of Verizon's officials and employees, and that knowledge may consist of nothing more than network design information or software access information.

"Graymail" is a practice by criminal defendants in which the defendant seeks to avoid prosecution by threatening to disclose classified materials in open court.[97] Congress enacted a statute to deal with this problem, the Classified Information Procedures Act (CIPA).[98] Under CIPA, when it appears that classified information may be disclosed in a criminal case, any party may move for a pretrial conference to consider rules for discovery and disclosure of that

---

94. 18 U.S.C. § 798(a)(1) prohibits making available to an unauthorized person any "classified information" relating to the "communications intelligence activities of the United States."

95. DOJ letter filed 7/31/06 at 4-5.

96. DOJ letter at 5.

97. In these cases the USG is often already a party.

98. 18 U.S.C.A. App. §§ 1-16.

information.[99] A defendant may not disclose classified information at trial without giving advance notice to the Attorney General,[100] who can then request a hearing to protect the information.[101] The court must conduct a hearing if one is requested, and the hearing may be held *in camera.*[102] Where a defendant seeks and ultimately receives classified information, the court can enter an order preventing further disclosure.[103] When the Attorney General submits an affidavit certifying that information is classified, the court may authorize the government to submit redacted documents, to submit summaries of documents, or to admit relevant facts.[104]

Under CIPA, court personnel have access to classified information. To facilitate this process, the Chief Justice of the United States has determined that no security clearances are required for judges, and security clearances have been sought for other court personnel.[105] The government can even compel defense counsel to undergo a DOJ initiated security clearance procedure,[106] and classified information can be provided to the defendant's counsel.[107]

Like CIPA, these dockets present a conflict between a party's rights (and need for evidence to exert those rights) and the government's need to keep the information from disclosure because of its potential harm to national security interests.[108] We find it instructive that CIPA allows a criminal court wide latitude to balance these interests and to use tools such as security clearances, closed hearings, redaction, summaries and protective orders. We also find it instructive that the government in CIPA cases has offered (and even mandated) security clearances for criminal defense counsel. It is disappointing that the USG has not offered to use any such limiting techniques in this proceeding. Nevertheless, CIPA does not apply here. While we might wish the law were otherwise, we have no legal authority to insist upon CIPA-like

---

99. *See* 18 U.S.C.A. App. § 2.
100. *See* 18 U.S.C.A. App. § 5(a).
101. *See* 18 U.S.C.A. App. § 6(a).
102. *See* 18 U.S.C.A. App. § 6(a).
103. *See* 18 U.S.C.A. App. § 3.
104. *See* 18 U.S.C.A. App. § 6(c)(2).
105. *U.S. v. Jolliff*, 548 F.Supp. 229, 231 (D. Md. 1981).
106. *U.S. v. Bin Laden*, 58 F.Supp.2d 113 (S.D.N.Y. 1999).
107. *Jolliff*, *Bin Laden*, above.
108. CIPA also involves other constitutional rights such as the right to assistance of counsel and the right to confront adverse witnesses in criminal cases.

procedures. Yet, it is unfortunate that thousands of Vermont's citizens' right to privacy does not receive similar procedural protection.

The issue here, therefore, is whether we should deny relief to the petitioners in this proceeding because the petitions seek information that may be classified. In deciding this question, we return again to the key fact that there is no sworn evidence or affidavits on any of these matters. We conclude that there is no evidentiary basis to find that federal classification systems will prevent us from reaching a decision in these matters. Unlike CIPA cases in which the government must present an affidavit opposing release of classified information, here we have only a letter and a photocopy of an affidavit submitted elsewhere. This does not provide an adequate basis to dismiss the petitions.

In addition, as we did above, we rely on the possibility of future disclosures. As the *Hepting* court found, reliable public disclosures between now and the time that this case is decided may allow petitioners to establish a right to relief independent of classified information.

Intelligence Reform and Terrorism Prevention Act of 2004

The USG asserts that requiring Verizon to reply to discovery in these dockets would violate the Intelligence Reform and Terrorism Prevention Act of 2004.[109] This statute gives the Director of National Intelligence ("DNI") the authority to "protect intelligence sources and methods from unauthorized disclosure."[110]

This statute is clear on its face. It imposes a duty on the DNI, not on this Board. One might argue that this statute obligates the DNI to intervene in these proceedings to protect intelligence sources. It might even be arguable that this statute gives the DNI a defense to an action seeking disclosure of information he holds. The statute clearly does not, however, create a duty for this Board to dismiss dockets brought by customers and the Department against a utility.[111] It certainly does not require us to do so without receiving evidence that draws a connection between the evidence sought and the sworn evidence that this intrudes upon the government's intelligence sources and methods.

---

109. DOJ letter at 4.

110. Pub. L. No. 108-458, 118 State. 3638 (Dec. 17, 2004), codified at 50 U.S.C. § 403-1(i)(1).

111. *Terkel*, slip op. at 12.

Other Procedural Motions

As noted above, Michael Bandler moved on August 15 to alter the schedule in light of the failure of the USG to send copies of the DOJ letter to the parties. On August 18, based on a previous motion, we issued an Order responding to an earlier similar motion from Mr. Bandler and giving the parties until August 25 to file comments on the DOJs letter that was filed here on July 31. While we may not approve of the USG sending a letter in this docket without copying the parties, the USG is not a party here, and we do not have authority to impose any sanctions for violation of our procedural rules. Any harm to the other parties has been remedied by the passage of time and by the opportunity, granted in the August 18 Order, to file supplemental comments. The Bandler motion to reschedule is denied.

Mr. Bandler also filed a motion seeking to expand the scope of this docket to Verizon's interactions with "data brokers." These private recipients of data were not a part of the original petition, but the same privacy interests are involved. If customer call records are disclosed to private investigative agencies, that can be every bit as much a concern to Vermont ratepayers as disclosure to the United States government. The parties are free to conduct discovery and submit testimony on this point.

III. CONCLUSION

We deny Verizon's Motion to Dismiss because there is the possibility that facts will be adduced to sustain petitioners' claims. We recognize that the parties may now seek discovery of a sort recently prohibited by two federal district courts. However, we believe that the better approach is to limit discovery on a more particularized basis.

The parties may seek evidence on whether Verizon has provided local calling records to the NSA, whether Verizon provided information to the NSA before February, 2006, and the conditions under which Verizon provides access to its customer records.

SO ORDERED.

Dated at Montpelier, Vermont, this 18th day of September, 2006.

s/ James Volz	)	
	)	PUBLIC SERVICE
	)	
s/ David C. Coen	)	BOARD
	)	
	)	OF VERMONT
s/ John D. Burke	)	

OFFICE OF THE CLERK

FILED: September 18, 2006

ATTEST: s/ Susan M. Hudson
Clerk of the Board

NOTICE TO READERS: This decision is subject to revision of technical errors. Readers are requested to notify the Clerk of the Board (by e-mail, telephone, or in writing) of any apparent errors, in order that any necessary corrections may be made. (E-mail address: psb.clerk@state.vt.us)